UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

One Plus 6T cellular phone with IMEI 865208042250392 that is black in color. The SUBJECT DEVICE is currently located at the HSI office, 9875 Redhill Drive, Blue Ash, Ohio, 45242

Case No. 1:20-mj-942

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 2251(a) and (e) and 2252(a) and 2252(A)	Illegal production, distribution, receipt and possession of child pornography.

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Christopher Wallace, Special Agent, HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by via FaceTime video *(specify reliab*

Date: Dec 28, 2020

Karen L. Litkovitz
United States Magistrate Judge

City and state: Cincinnati, OH

ATTACHMENT A

The property to be searched is a One Plus 6T cellular phone with IMEI 865208042250392 that is black in color. The SUBJECT DEVICE is currently located at the HSI office, 9875 Redhill Drive, Blue Ash, Ohio, 45242.

This warrant authorizes the forensic examination of SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. SUBJECT DEVICE as described in Attachment A that relates to 2252(a)(2)s of 18 U.S.C. §§2252(a)(2)(B) and 2252A(a)(2); and 18 U.S.C. §§2252(a)(4)(B)and 2252A(a)(5)(B) involving Mark BEAULIEU ("BEAULIEU"), including:

    a. Any Internet or cellular telephone communications (including email, social media, online chat programs, and text messages) with minors (as defined in 18 U.S.C. § 2256(1), *i.e.*, individuals under the age of 18), and any contact/identifying information for these individuals;

    b. Communication regarding the acquisition or dissemination of child pornography;

    c. Any visual depictions and records related to the possession, receipt, distribution, and production of child pornography or child erotica;

    d. Records and information relating to the identify or identification of any victim or potential victims;

    e. Evidence of utilization of email accounts, social media accounts (including but not limited to, information regarding BEAULIEU's access to Instagram, Grinder Facebook, and KIK), online chat programs, and Peer-to-Peer sharing programs, including any account/user names;

    f. Records and information relating to identification of any additional participants in the scheme;

    g. Any photography, videos or other visual depictions of minors, including, but not limited to child pornography as defined in 18 § U.S.C. 2256(8) and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica;

    h. Evidence regarding BEAULIEU's travel, including but not limited to credit card receipts, itineraries/maps/driving directions, GPS information, and hotel reservations/bills;

    i. Any evidence relating to BEAULIEU's solicitation (or attempted solicitation) of or meeting (or attempted meeting) with minors to engage in sexual activity, including but not limited to the production and/or solicitation of nude photographs and/or videos of minors;

    j. Information regarding access to websites or other internet platforms where child pornography is distributed, including any Internet history indicative of searching for child pornography;

    k. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages,

and other digital files) that concern any accounts with an Internet Service Provider;

l. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE;

m. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE;

n. Records of or information about Internet Protocol addresses used by SUBJECT DEVICE;

o. Records of or information about SUBJECT DEVICE Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

p. Evidence of utilization of aliases and fictitious names.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data), any photographic and video form.

ATTACHMENT C

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B)	Receipt or Distribution of Child Pornography
18 U.S.C. §2252A(a)(2)	Receipt or Distribution of Child Pornography

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Christopher Wallace, being duly sworn, depose and state the following:

INTRODUCTION

1. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — one electronic device, described in Attachment A — which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent (SA) with Immigration and Customs Enforcement, Homeland Security Investigations (HSI) and have been so employed since May 2005. I am currently assigned to the HSI Resident Agent in Charge Cincinnati, Ohio office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§2251(a) and (e), 2252(a), and 2252A). I have received training related to the investigation of sexual exploitation of children offenses and the recovery of evidence.

3. Along with other agents and officers of HSI, I am currently involved in an investigation of child pornography and child exploitation offenses committed by Mark BEAULIEU (hereinafter referred to as "BEAULIEU"). This Affidavit is submitted in support of an Application for a search warrant for the following:

   a. One Plus 6T cellular telephone bearing IMEI 865208042250392, black in color, currently located at the HSI office, 9875 Redhill Drive, Blue Ash, Ohio, 45242 (hereinafter referred to as "SUBJECT DEVICE");

4. The electronic device listed above is more fully described in Attachment A. The purpose of the Application is to seize evidence of violations of 18 U.S.C. § 2252(a)(2)(B) and 18 U.S.C. § 2252A(a)(2), which make it a crime to receive/distribute or attempt to receive/distribute child pornography, and 18 U.S.C. §§2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography. The applied-for warrant would authorize the forensic examination of SUBJECT DEVICE for the purpose of identifying electronically stored data particularly described in Attachment B.

5. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents and officers involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

6. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the search of SUBJECT DEVICE.

7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal law, including 18 U.S.C. §§2252(a)(2)(B) and (a)(4)(B), 2252A(a)(2) and (a)(5)(B), are present on SUBJECT DEVICE.

PERTINENT FEDERAL CRIMINAL STATUTES

8. 18 U.S.C. § 2252(a)(2)(B) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mail if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

9. 18 U.S.C. § 2252A(a)(2) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce, shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

10. 18 U.S.C. § 2252(a)(4)(B) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

11. 18 U.S.C. § 2252A(a)(5)(B) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

Definitions

12. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

a. "**Child Pornography**" includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

b. "**Visual depictions**" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

c. "**Minor**" means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).

d. "**Sexually explicit conduct**" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. §§ 2256(2) and 1466A(f)).

e. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

f. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-

up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

g. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

h. **"Wi-Fi"** is a technology that allows electronic devices to connect to a wireless LAN network. Devices that use Wi-Fi technology include personal computers, video game consoles, smartphones, digital cameras, tablets, and modern computers.

i. A "**wireless telephone"** (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

j. A "**SMS**" (short message service) is a technology for sending short text messages between telephones.

k. A "**MMS**" (multimedia message service) is a method of transmitting graphics, video or sound files, and short text messages over wireless networks such as mobile telephones.

l. A "**digital camera**" is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various

types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

m. A "**GPS**" navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

n. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Use of Computers and the Internet with Child Pornography

13. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.

a. **Production**. Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The

output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc*.) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.

b. **Communication**. Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.

c. **Distribution**. Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.

d. **Storage**. The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of

these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

FACTS SUPPORTING PROBABLE CAUSE

14. Kik Interactive, Inc., an electronic service provider, provided reports of Child Sexual Abuse Material (CSAM) to the Royal Canadian Mounted Police (RCMP), which were discovered on its platform. The RCMP filtered the content and provided referrals relating to the respective Kik account users to Homeland Security Investigations (HSI) Cyber Crimes Center (C3). HSI C3 then disseminated leads to HSI domestic offices.

15. On or about September 16, 2019, HSI Cincinnati received a lead from HSI C3 associated with an uploaded image of child pornography by Kik username: "sf2034". On April 23, 2019, Kik username: "sf2034" uploaded an image of child pornography from the IP address 216.68.149.58.

a. The image depicts a prepubescent female posing on a beach. The prepubescent female is visible from head to toe in the image. The female is standing naked and the breasts and vagina are clearly visible.

16. According to Kik's records, the subscriber information for username: sf2034 also included the following pertinent information:
a. First Name: Sam
b. Last Name: Longford
c. DOB: 4/17/1998
d. Device Type: ONEPLUS A6013 (advertised as the Oneplus 6T)
e. Kik username: sf2034 also logged in from IP address 65.27.132.189 on April 23, 2019

17. A query of a public online database revealed that IP address 216.68.149.58 is registered to Fuse Internet (Cincinnati Bell). On September 16, 2019, HSI Cincinnati issued a summons to Fuse Internet (Cincinnati Bell) for the subscriber of IP address 216.68.149.58 on April 23, 2019. Fuse provided the subscriber information as Amp Electric Vehicles; 100 Commerce Drive, Loveland, Ohio.

18. A query of a public online database revealed that IP address 65.27.132.189 is registered to Charter Communications. On September 30, 2019, HSI Cincinnati issued a summons to Charter Communications for the subscriber of IP address 65.27.132.189 on April 23, 2019. Charter provided the subscriber information as Mark BEAULIEU; 4828 Fairview Ave, Apt 2, Blue Ash, Ohio.

19. On December 15, 2020, SA Christopher Wallace and SA Kim Wallace spoke with a human resources representative of Workhorse Headquarters (Formerly AMP Electric Vehicles). They confirmed that BEAULIEU is currently working at Workhorse Headquarters and has been for approximately five (5) years. SA Christopher Wallace left a business card with the HR representative and asked that the HR representative have BEAULIEU contact SA Christopher Wallace.

20. On December 18, 2020, BEAULIEU contacted SA Christopher Wallace by phone. SA Christopher Wallace asked BEAULIEU when would be a good time to speak with BEAULIEU and offered to come to BEAULIEU's residence in Blue Ash. BEAULIEU responded that he (BEAULIEU) would prefer to come to the HSI office in Blue Ash. SA Christopher Wallace agreed and an appointment was set for December 21, 2020.

21. On December 21, 2020, SA Christopher Wallace and SA Kim Wallace spoke with BEAULIEU in a conference room at the HSI office. At the onset of the consensual interview, BEAULIEU took out his (BEAULIEU) One Plus cellular phone and placed the cellular phone on the table without being asked to do so. During the consensual interview BEAULIEU confirmed that he (BEAULIEU) has worked at Workhorse Headquarters for approximately five (5) years and that there is a wifi network available for the employees at Workhorse Headquarters to use. BEAULIEU also confirmed that he (BEAULIEU) is currently residing at 4828 Fairview Avenue, Apartment 2 in Blue Ash, Ohio. BEAULIEU also admitted to having used the Kik application in the past and possibly in April of 2019, but denied ever uploading child pornography to the Kik application. SA Christopher Wallace asked BEAULIEU for permission to forensically examine BEAULIEU's One Plus cellular phone, but BEAULIEU refused.

22. Agents then took possession of the SUBJECT DEVICE and placed SUBJECT DEVICE into airplane mode in order to preserve evidence.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

24. There is probable cause to believe that things that were once stored on SUBJECT DEVICE may still be stored there, for at least the following reasons:

    a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file

on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described in the warrant, but also forensic evidence that establishes how SUBJECT DEVICE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on SUBJECT DEVICE because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of criminal offenses may be located on SUBJECT DEVICE, in violation of 18 U.S.C. §§2252(a)(2)(B) and 2252A(a)(2); and 18 U.S.C. §§2252(a)(4)(B) and 2252A(a)(5)(B).

29. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Respectfully submitted,

_____

Christopher Wallace
Special Agent
Homeland Security Investigations

SUBSCRIBED and SWORN
before me this 28th day of December 2020

Karen L. Litkovitz
United States Magistrate Judge

ATTACHMENT A

The property to be searched is a One Plus 6T cellular phone with IMEI 865208042250392 that is black in color. The SUBJECT DEVICE is currently located at the HSI office, 9875 Redhill Drive, Blue Ash, Ohio, 45242.

This warrant authorizes the forensic examination of SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. SUBJECT DEVICE as described in Attachment A that relates to 2252(a)(2)s of 18 U.S.C. §§2252(a)(2)(B) and 2252A(a)(2); and 18 U.S.C. §§2252(a)(4)(B)and 2252A(a)(5)(B) involving Mark BEAULIEU ("BEAULIEU"), including:

    a. Any Internet or cellular telephone communications (including email, social media, online chat programs, and text messages) with minors (as defined in 18 U.S.C. § 2256(1), *i.e.*, individuals under the age of 18), and any contact/identifying information for these individuals;

    b. Communication regarding the acquisition or dissemination of child pornography;

    c. Any visual depictions and records related to the possession, receipt, distribution, and production of child pornography or child erotica;

    d. Records and information relating to the identify or identification of any victim or potential victims;

    e. Evidence of utilization of email accounts, social media accounts (including but not limited to, information regarding BEAULIEU's access to Instagram, Grinder Facebook, and KIK), online chat programs, and Peer-to-Peer sharing programs, including any account/user names;

    f. Records and information relating to identification of any additional participants in the scheme;

    g. Any photography, videos or other visual depictions of minors, including, but not limited to child pornography as defined in 18 § U.S.C. 2256(8) and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica;

    h. Evidence regarding BEAULIEU's travel, including but not limited to credit card receipts, itineraries/maps/driving directions, GPS information, and hotel reservations/bills;

    i. Any evidence relating to BEAULIEU's solicitation (or attempted solicitation) of or meeting (or attempted meeting) with minors to engage in sexual activity, including but not limited to the production and/or solicitation of nude photographs and/or videos of minors;

    j. Information regarding access to websites or other internet platforms where child pornography is distributed, including any Internet history indicative of searching for child pornography;

    k. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages,

and other digital files) that concern any accounts with an Internet Service Provider;

l. Passwords, encryption keys, and other access devices that may be necessary to access SUBJECT DEVICE;

m. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from SUBJECT DEVICE;

n. Records of or information about Internet Protocol addresses used by SUBJECT DEVICE;

o. Records of or information about SUBJECT DEVICE Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

p. Evidence of utilization of aliases and fictitious names.

2. Evidence of user attribution showing who used or owned SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data), any photographic and video form.

ATTACHMENT C

Code Section	Offense Description
18 U.S.C. §2252(a)(4)(B)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B)	Receipt or Distribution of Child Pornography
18 U.S.C. §2252A(a)(2)	Receipt or Distribution of Child Pornography